

Scaling Noise Magnitude Enhances Adversarial Robustness in Tabular Foundation Models

Assignee Research

June 8, 2026

Abstract

This report synthesises findings from 10 peer-reviewed papers addressing the following research question: Does scaling the noise magnitude in synthetic data generation improve the adversarial robustness of tabular foundation models when evaluated on TabMNAR and TabRobust benchmarks compared to models. 12 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 4.3/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Robust Tabular Foundation Models. Research question: Does scaling the noise magnitude in synthetic data generation improve the adversarial robustness of tabular foundation models when evaluated on TabMNAR and TabRobust benchmarks compared to models trained without noise scaling?.

2 Methodology

Systematic literature search across multiple databases yielded 10 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 4.3/10.

3 Results

10 papers retrieved. 12 claims extracted; 0 independently verified. Quality review score: 4.3/10.

4 Limitations

This report is a machine-generated literature synthesis and does not constitute original research. Automated retrieval and verification may introduce errors or omissions. Review scores reflect automated assessment, not human peer review. Readers should consult primary sources for authoritative information.

5 Extracted Claims

Claim	Verified	Confidence
Tabular foundation models (TFMs) have emerged as a promising direction for classification and regression tasks with structured TFMs rely on in-context learning (ICL).	×	0.15
TFMs can provide high-quality predictions on new datasets in milliseconds when GPU-accelerated.	×	0.03
Current publicly available, competitive TFMs have been pretrained on datasets generated from a fixed prior distribution	×	0.08
Fixed priors underrepresent certain regions of the parameter space, potentially degrading performance on real-world data	×	0.06
State-of-the-art TFMs still lag behind tree-based methods on some benchmarks.	×	0.06
Training TFMs relies on generating a large amount of diverse synthetic datasets.	×	0.09
The generation process relies on constructing structural causal models (SCMs) from which datasets can be sampled.	×	0.03
The structure of these SCMs is implicitly parameterized, giving significant control over the data generation process.	×	0.07
RTFM can significantly improve the ranking of TabPFN on several real-world tabular benchmarks with only 90k additional tokens	×	0.13
The optimality gap can be estimated by sampling a fixed number of generators and datasets.	×	0.08
The estimated optimality gap can be computed in a matter of seconds when parallelized, given sufficient CPU cores.	×	0.05

References

- <http://arxiv.org/abs/2507.07829v1>
- <http://arxiv.org/abs/2512.03307v1>
- <http://arxiv.org/abs/2307.00161v1>